

REMARKS

A. Preliminary Discussion

In a telephone call initiated by the Examiner, applicant's attorney of record elected with traverse to prosecute the claims in Group XI constituting claims 115-121, 145-150, 159-183 and 187-191. Applicant subsequently filed a preliminary amendment in which applicant amended claims 115-121, 145-150, 159-183 and 187-191 and added claims 226-242.

Thereafter, applicant received an Office Action dated 05/20/2004. In this Office Action, the Examiner rejected all of claims 115-121, 145-150, 159-183, 187-191 and 226-242 either under 35 U.S.C. 103 as anticipated by Barkan EPO patent application WO98/17042 or under 35 U.S.C. 103(a) on the basis of Barkan in view of Zabetian patent 6,327,656.

Applicant filed an amendment in response to the Office Action dated 05/20/2004. Thereafter, the USPTO issued a Notice of Non-Compliant Amendment (37 CFR 1.121) on 10/08/2004. This Supplemental Amendment is in response to the Notice of Non-compliant Amendment. In this Supplemental Amendment, applicant has included all of the claims in the application. Applicant has also included a request that any fee in connection with the filing of this amendment should be taken from Account No. 06-2425.

Applicant has revised claims 146 and 147 to overcome the objections of the Examiner. Applicant has also made changes in a number of the claims to overcome informalities noted by applicant's attorney in a further study of the claims to prepare this amendment.

In this amendment, applicant has retained claims 115-121, 145-150, 159-183, 187-191 and 226-242, all of them in at least somewhat amended form, and has added claims 243-285 by this amendment. As now written, all of the claims in the application are believed to be definite.

Applicant respectfully submits that all of the claims in this application as written before the Office Action dated 05/20/04 are allowable over (a) Barkan alone and (b) Barkan in view of Zabetian. However, applicant has made changes in claims 115-121, 145-150, 159-183, 187-191 and 223-242 to sharpen the patentable distinctions between applicant's invention as now recited in the claims and the cited references to reinforce the allowability of applicant's claims over the cited references.

B. An Analysis of the Inapplicability of the Prior Art References Against

Applicant's claims

1. Barkan EPO application WO98/17042

a. There is an extremely important reason, among a number of important reasons, why Barkan does not constitute a proper reference against applicant's claims. Applicant may be considered illustratively to provide a combination of elements A, B, C, D, E. This combination may be considered to be streamlined relative to a combination illustratively constituting elements A, F, B, G, C, H, D, I, E, J in Barkan. The elements F, G, H, I and J in Barkan may be considered to constitute the steps in which the message is encrypted and in which the mail server 3 in Figure 1 of Barkan discloses to the sender the key individual to the recipient and in which the mail server 3 discloses to the recipient

the key individual to the sender. The encrypted message is transmitted by the sender to the mail server 3 in Barkan so that the sender can first learn of the encryption key at the recipient (e.g. step F). The sender can then use the encryption key to send an encrypted message to the recipient (e.g., step G). When the sender sends an encrypted message to the recipient, the encrypted message is further encrypted with the recipient's encryption key (e.g., Step H) and the recipient uses the recipient's key to decrypt the encrypted message. The recipient can then send a message to the mail server 3 to learn of an encryption key individual to the sender (e.g., Step I). The recipient then uses the sender's encryption key to send a message to the sender (e.g., Step J). These steps are not included in applicant's method. It will be appreciated that other steps are disclosed in Barkan in addition to illustrative steps F, G, H, I and J as illustratively described above and that these other steps are not provided by applicant.

The Examiner has illustratively eliminated the steps F, G, H, I and J in citing Barkan against applicant's claims. By illustratively eliminating the steps F, G, H, I and J in Barkan, the Examiner theoretically may possibly obtain a combination of A, B, C, D and E in Barkan (without the steps F, G, H, I and J in Barkan). However, the pared down system constituting the steps A, B, C, D and E is inoperative.

It is not proper for the Examiner to reject applicant's claims on the basis of an inoperative combination of elements in Barkan. Applicant would accordingly appreciate it if the Examiner would reconsider his rejection of the claims on the basis of Barkan alone or Barkan in combination with Zabetian.

Applicant respectfully suggests that the Examiner should allow applicant's claims if the Examiner cannot find prior art references more appropriate, and more significant, than Barkan. In other words, in order to reject applicant's claims, the Examiner should have to cite a reference directly disclosing the steps A, B, C, D and E and without any intermediate step between A and B, any intermediate step between B and C, etc. At any rate, it is well recognized that, if applicant recites a method including steps A, B, C, D and E, the claim is allowable over a prior art method illustratively constituting steps A, F, B, G, C, H, etc., particularly if applicant provides distinct advantages over the system that includes steps F, G, H, etc.

b. Barkan discloses eight (8) different methods. There is very little, if any, commonality between the different methods with respect to the specific method steps in the different methods. It is accordingly not appropriate for the Examiner to reject a claim on the basis that a first method in Barkan discloses some, but not all, of the steps recited in the claim and another method in Barkan discloses other steps, but not all, of the steps recited in the claim. In order for the Examiner to reject a claim on the basis of Barkan, the Examiner has to apply the same method in Barkan against all of the steps recited in the claim. Furthermore, as indicated in subsection (A)(1)(a) immediately above, the steps cited by the Examiner in the selected method of Barkan have to appear as successive steps in the claim.

c. Each of Barkan's eight (8) methods is considerably more complicated than applicant's method. One reason is that each of the sender and the recipient in Barkan has a key that is different from the key of the other one of the sender

and the recipient and is individual to the selected one of the sender and the receiver. In order to reconcile this difference, Barkan provides an intermediate station (mail server 3 in Figure 1 of Barkan) and sometimes intermediate servers. The intermediate server (or servers) in Barkan inform(s) the sender of the recipient's key and informs the recipient of the sender's key. The sender's key is represented by first encryptions and the recipient's key is represented by second encryptions different from the first encryptions. The sender does not initially know the recipient's key and has to obtain this information from the mail server 3. This involves considerably more steps of communication than in applicant's system.

In applicant's system, the sender and the recipient do not have any keys. This allows the RPOST server in applicant's system to communicate directly with the recipient on an unencrypted basis. This is much more simple, direct, accurate and faster than Barkan is able to provide since Barkan's system is more complicated.

Applicant has amended the claims to recite that the RPOST server in applicant's system provides an unencrypted message to the destination server constituting the recipient. This recitation or similar recitations appear in all of applicant's claims. Because of this, applicant's system is faster, more accurate, more simple, more direct and more reliable than Barkan's system. The communication of an unencrypted message by the RPOST server to the destination server provides a sharp and patentable distinction over Barkan. This distinction is enough in itself to cause all of the applicant's claims to be allowable over Barkan.

d. In applicant's invention, the message is never encrypted. It is true that applicant produces a digital signature (a hashed encryption) of the unencrypted message before applicant transmits the message and the digital signature of the message to the sender. But this digital signature is in addition to the unencrypted message and not in place of the unencrypted message as in Barkan. This is also true of applicant's unencrypted attachment since applicant's server sends the attachment and the digital signature (the hashed encryption) of the unencrypted attachment to the sender. Because there is no encrypted message in applicant's system, the RPOST server in the RPOST system can communicate easily and immediately (without any intermediate steps) with the sender.

In contrast, as a first step, or one of the first steps in his methods, Barkan encrypts the message. Sometimes Barkan even adds more than one (1) layer of encryption to the message. Sometimes, the encryption may constitute as many as three (3) layers (see Figure 4 of Barkan). These encryptions in Barkan unduly complicate, and reduce the speed of, the operation of Barkan's system, particularly when compared to the simplicity of applicant's system. One reason for the complication is that a first encryption provides a first key individual to the sender and a second encryption provides a second key individual to the recipient. The sender has to request the mail server 3 in Figure 1 of Barkan to obtain the recipient's key and the recipient has to request the mail server 3 for the sender's key.

e. In Barkan, the message is encrypted before it is transmitted to

the recipient. Because of this, the sender has to inform the recipient through the mail server 3 (or servers) of the encryption code that the sender is using in communicating the encrypted message through the intermediate mail server 3 (or intermediate servers) to the recipient. In like manner, the recipient has to notify the sender through the mail server 3 (or intermediate servers) of the encryption code that the recipient is using so that the sender will be able to decrypt the encrypted communication from the recipient.

In applicant's invention, the message is encrypted after the message has been transmitted by the RPOST server to the destination address and has been received at the destination address. As the Examiner will see from the above discussion, each of the eight (8) Barkan methods in Barkan is considerably more complicated than applicant's method. This considerably slows the time in Barkan for transmitting a message from the sender to the recipient. It also provides an increase in the production of errors in Barkan's system in comparison to applicant's system.

In RPOST's method, no encryption of the unencrypted message is provided by applicant's server until after the message has been delivered to the destination address. After the message has been transmitted to the destination address and applicant's server has been apprised of this transmittal, applicant then produces a digital signature (an encrypted hash) of the message. However, applicant retains the unencrypted message without any encryption even after applicant hashes and encrypts the unencrypted message. This hatched encryption is provided by RPOST to authenticate the message. Applicant then sends the unencrypted message and the digital signature of the unencrypted message to the sender.

Barkan does not operate with an unencrypted message. Furthermore, to authenticate the encrypted message, Barkan does not use the unencrypted message and the digital signature of the unencrypted message.

Barkan produces an encryption and sometimes two encryptions (one layered on the other) of the message (see Figure 3 of Barkan). Furthermore, Barkan sometimes even produces three (3) layers of encryption. (See Figure 4 of Barkan). Barkan produces a hash or an encryption of the message but Barkan does not produce a hashed encryption of the message.

Because Barkan does not produce a hashed encryption of the message but produces an encryption of the unencrypted message, Barkan cannot provide an authentication of the message in the same manner that RPOST provides in its system. The reason is that applicant operates on the unencrypted message and the digital signature of the unencrypted message to produce a pair of digital fingerprints (hashes) of the message. Applicant compares the digital fingerprints to authenticate the unencrypted message.

Since Barkan does not provide a hashed encryption (digital signature) of the unencrypted message, Barkan cannot provide a digital fingerprint (hash) of the digital signature. Barkan cannot accordingly operate on the unencrypted message and the hashed encryption (the digital signature) to produce two (2) digital fingerprints (hashes) of the message. Barkan cannot compare two (2) digital fingerprints of the message to authenticate the message.

f. There are other significant differences between RPOST's invention and Barkan. These differences are recited in applicant's claims. For example, when applicant's server sends the unencrypted message to the destination address, the unencrypted message often passes through intermediate stations between applicant's server and the destination address to reach the destination address. An indication is provided of the arrival of the message at the destination server through the set of intermediate stations. The same set or another set of intermediate stations may be provided to reach applicant's server from the destination address. The passage of information through intermediate stations between applicant's server and the destination address constitutes an attachment. The attachment is not encrypted. Applicant produces a digital signature (hashed encryption) of the attachment and sends the unencrypted attachment and the digital signature of the attachment to the sender. Applicant then discards or destroys the digital attachment and the digital signature of the digital attachment.

To obtain a further authentication of the unencrypted message, the sender sends the unencrypted attachment and the digital signature of the unencrypted attachment to applicant's server. Applicant's server then operates on the unencrypted attachment and the digital signature of the unencrypted attachment to authenticate the unencrypted attachment. In authenticating the unencrypted attachment, applicant in effect provides a further authentication of the unencrypted message.

Barkan does not provide an attachment corresponding to applicant's attachment and does not actually even provide what can be considered to be an attachment. Since

Barkan does not provide an attachment, Barkan cannot provide a digital signature of the attachment. The failure of Barkan to provide an attachment and a digital signature of the attachment prevents Barkan from authenticating the attachment. This prevents Barkan from using an attachment to verify an authentication of a message.

g. As will be seen, Barkan does not disclose the creation of a digital signature in any of his eight (8) methods. This applies not only to a digital signature of a message but also to a digital signature of an attachment. This prevents Barkan from producing a digital fingerprint (a hash) of the message and a decryption (the hash) of the digital signature. Thus, Barkan does not compare two (2) digital fingerprints to authenticate an attachment. This is what applicant does.

h. If the Examiner were to cite the combination of AFBGCHDIEJ against applicant's claims because this combination includes the steps ABCDE, applicant's claims would still be allowable over Barkan. It is well recognized that an invention is patentable when the invention relates to a series of steps considerably simplified from a series of steps known in the prior art. This is particularly true when the simplified series of steps produces results better and faster and more reliable than the complex series of steps of the prior art.

i. Applicant discards or destroys the unencrypted message and the digital signature of the unencrypted message after the transmission of the unencrypted message and the digital signature of the unencrypted message by the server to the sender. Applicant also discards or destroys the unencrypted attachment and the digital signature

of the unencrypted attachment after the transmission of the unencrypted attachment and the digital signature of the unencrypted attachment by the server to the sender.

Barkan does not do this.

j. Without encrypting the unencrypted message, applicant provides a digital fingerprint of the unencrypted message and a digital fingerprint of the digital signature of the unencrypted message. Applicant then compares the digital fingerprints to authenticate the unencrypted message.

Also without encrypting the unencrypted attachment, applicant provides a digital fingerprint of the unencrypted attachment and a digital fingerprint of the digital signature of the unencrypted attachment. Applicant then compares the two (2) fingerprints relating to the message to authenticate the message. Applicant then compares the two (2) fingerprints relating to the attachment to authenticate the attachment. Authenticating the attachment may be considered to provide a further authentication of the message.

Barkan does not disclose any of the steps specified in subsection k and performed by applicant.

k. In applicant's system, the server receives an unencrypted attachment without encrypting the unencrypted message or the unencrypted attachment. The server then provides a digital signature of the unencrypted attachment without encrypting the unencrypted message or the unencrypted attachment. The server then transmits to the sender the unencrypted attachment and the digital signature of the unencrypted attachment without encrypting the unencrypted attachment.

Barkan does not disclose this.

1. Without encrypting the unencrypted message and the unencrypted attachment, the server receives from the sender the unencrypted message and the unencrypted attachment and the digital signatures of the unencrypted message and the unencrypted attachment. The server generates digital fingerprints of the unencrypted message and the unencrypted attachment and digital fingerprints of the digital signatures of the unencrypted message and the unencrypted attachment. The server compares the digital fingerprints of the unencrypted message and the digital signature of the unencrypted message, and compares the digital fingerprints of the unencrypted attachment and the digital signature of the unencrypted attachment, to authenticate the unencrypted message and the unencrypted attachment.

Barkan does not disclose this.

- m. The destination address is one of a plurality of destination addresses receiving the unencrypted message from the server. The server distinguishes each of the destination addresses in the transmission of the unencrypted message to the destination addresses. In this way, each destination address is identified differently from the other destination address.

Barkan does not disclose this.

- o. The path of transmission of the unencrypted message between the server and the destination address includes the identity and address of the server and the identity and address of a recipient at the destination address.

Barkan does not disclose this.

p. Applicant transmits the unencrypted message from the server to the destination address via a protocol selected from the group consisting of an SMTP protocol and an ESMTP protocol without encrypting the unencrypted message. Applicant receives at the server the transmission of the unencrypted message between the server and the destination address via the selected one of the SMTP and the ESMTP protocols without encrypting the unencrypted electronic message.

Barkan does not disclose this.

q. Without encrypting the unencrypted message, applicant records, in the transmission between the server and the destination address, the time for the transmission of the unencrypted message from the server to the destination address and the time for the receipt of the unencrypted message at the destination address.

Barkan does not disclose this.

r. Applicant includes, in the transmission of the unencrypted message between the server and the destination address via the selected one of the SMTP and ESMTP protocols, the status of the delivery of the unencrypted message at the destination address without encrypting the unencrypted message.

Barkan does not disclose this.

s. Applicant transmits the unencrypted message from the server to a designated address via a particular protocol without encrypting the unencrypted message. Without encrypting the unencrypted message, applicant receives at the server the transmission of the unencrypted message between the server and the

designated address via the particular protocol without encrypting the unencrypted message.

Barkan does not do this.

t. In a method of authenticating an unencrypted message provided by a sender and transmitted to a destination server by a second server displaced from the sender and the destination server, applicant provides an unencrypted attachment transmitted between the second server and the destination address via a selected one of SMTP and ESMTP protocols without encrypting the unencrypted message or the unencrypted attachment. Applicant then transmits the unencrypted attachment from the second server to the sender without encrypting the unencrypted attachment.

Barkan does not disclose this.

u. Applicant provides for the transmission from the server to the sender of the unencrypted message and the unencrypted attachment and a selected one of (a) a digital signature of the unencrypted message and a digital signature of the unencrypted attachment and (b) a digital signature of a combination of the unencrypted message and the unencrypted attachment. This transmission is provided without encrypting the unencrypted message and the unencrypted attachment.

Barkan does not disclose this.

v. Applicant provides at the server a digital signature of a combination of the unencrypted message and the unencrypted attachment. Without encrypting the unencrypted message and the unencrypted attachment, applicant transmits to the sender the unencrypted message and the unencrypted attachment and the digital

signature of the combination of the unencrypted message and the unencrypted attachment.

Barkan does not disclose this.

w. Applicant creates a fictitious address composed of a unique identifier of the unencrypted electronic message, a unique identifier of the destination address of the unencrypted electronic message and a domain name of a server, the fictitious address being designated as the Receipt Server.

Barkan does not disclose this.

x. Applicant adds to the unencrypted message a message header which directs a mail client of the recipient to send a notification message of the opening of the unencrypted electronic message.

Barkan does not disclose this.

y. Applicant receives, at the Receipt Server, a notification message of the opening of the unencrypted electronic message addressed to the fictitious address.

Barkan does not disclose this.

z. Applicant transmits the unencrypted electronic message through the internet to the recipient's mail client, the recipient's mail client being responsive to the unencrypted electronic message transmitted through the internet and being an e-mail server.

Barkan does not disclose this.

aa. Applicant provides a Delivery Status Notification for the unencrypted electronic message in compliance with the selected one of the SMTP protocol and the ESMTP protocol.

Barkan does not disclose this.

ab. The Receipt Server receives a notification message of the opening of the unencrypted electronic message addressed to the fictitious address.

Barkan does not disclose this.

2. Zabetian patent 6,327,656

Although applicant concedes that Zabetian discloses different protocols including the SMTP protocol, Zabetian does not disclose the steps specified above in subsections (B)(1)(a-g). In view of this, applicant's method as specified above is allowable over the combination of Barkan and Zabetian. Zabetian also does not disclose any of the steps recited in (B)(1)(h-ab).

The Examiner has cited Zabetian to show that documents using SMTP and ESMTP protocols have been transmitted in the prior art. The Examiner has then attempted to combine Zabetian with Barkan to reject applicant's claims. According to the Examiner, Barkan discloses all of the steps recited in applicant's claims except for the use of SMTP and ESMTP protocols. The Examiner then indicates that Zabetian discloses these protocols. The Examiner additionally contends that reciting the use of a selected one of the SMTP and ESMTP protocols for transmission of a message would have been obvious over Barkan in view of Zabetian to a person of ordinary skill in the art.

Applicant has never contended that applicant is the first to use SMTP and ESMTP protocols in a transmission of a message. Applicant does believe, however, that he is the first to use a selected one of SMTP and ESMTP protocols in authenticating a message transmitted on behalf of a sender to a recipient. Applicant also believes that he is the first to provide an attachment showing the transmission of the unencrypted message through intermediate stations between applicant's server and a destination address via a selected one of SMTP and ESMTP protocols to indicate an attachment including the intermediate stations. Applicant also believes that he is the first to use this attachment in providing an authentication of the unencrypted message transmitted to the destination address. Applicant does not believe that it would have been obvious at the time of applicant's invention to use applicant's authentication method to authenticate a message via a selected one of SMTP and ESMTP protocols. One proof of this is that no one prior to applicant has provided applicant's authentication method even though authentication techniques have been known and used for many years prior to applicant's invention.

The use by applicant of a selected one of the SMTP and ESMTP protocols provides certain additional advantages to applicant. Those advantages have not been previously known to persons of ordinary skill in the art. For example, the use by applicant of a selected one of the SMPT and ESMTP protocols provides a proof to the sender and the recipient that the message from the sender is received at the destination address of the recipient. This is independent of the authentication of this message sent by the sender to the destination address of the recipient.

The combination of Barkan and Zabetian to reject applicant's claims is particularly not appropriate because Zabetian does not disclose or suggest any of the methods specified above in subsections (B)(1)(a-b).

C. Analysis of the Reasons for the Allowability of Each Claim Over the Prior Art

Cited by the Examiner

In this section C, applicant will show why each of the claims being prosecuted in this application is allowable over the prior art cited by the Examiner whether the references are cited individually or in combination. Applicant will show this by reference to the analysis in subsection (B)(1)(a-ab).

All of claims 115-121, 145-150, 159-183, 187-191 and 220-260, are allowable over Barkan, and the combination of Barkan and Zabetian, for the reasons set forth in Subsections (B)(1)(a-e). One reason that the Examiner has cited Zabetian is because, according to the Examiner, Zabetian teaches that documents are transmitted between clients and servers by using conventional protocols such as the SMTP protocol. However, since neither Zabetian nor Barkan teaches what is discussed in subsections (B)(1)(a) – (B)(1)(e), all of the claims are allowable over the combination of Barkan and Zabetian for the reasons set forth in subsections (B)(1)(a) – (B)(1)e.

Starting with subsection (B)(1)(f) and extending through subsection (B)(1)(a-b), individual ones of the claims are allowable over Barkan, and the combination of Barkan and Zabetian, because the individual ones of the claims recite what is specified in that subsection and because the references do not disclose what is specified in that subsection.

Subsection (B)(1)(f)

Claims 115-121, 161, 169-171, 181, 182, 188, 189, 190, 227-229, 232, 233, 236, 237, 241, 242, 245, 246, 249, 250, 251, 252, 253, 254, 255, 256

Subsection (B)(1)(g)

Claims 119-120, 145-150, 173-178, 189-191, 226-229, 231-237, 238-242, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258

Subsection (B)(1)(h)

Claims 115-121, 182, 229, 236, 237, 241, 242, 246, 251, 252, 253, 255, 256

Subsection (B)(1)(i)

Claims 116, 117, 140, 168, 170, 239, 245, 248

Subsection (B)(1)(j)

Claims 121, 187, 191, 245.

Subsection (B)(1)(k)

Claims 117, 120, 182, 229, 236, 237, 241, 242, 246, 252, 253, 255, 256

Subsection (B)(1)(l)

Claims 118, 119, 120, 173-178, 227, 228, 229, 232, 23, 234, 235, 236, 237, 249, 250, 251, 252

Subsection (B)(1)(m)

Claims 120, 229, 236, 237, 251, 252

Subsection (B)(1)(n)

Claims 148, 150, 261, 262, 271, 276, 281

Subsection (B)(1)(o)

Claims 118, 160, 176, 178

Subsection (B)(1)(p)

Claims 159-165, 166-172, 173-178, 179-182, 183, 187-190, 226-229, 265,
266, 270-274

Subsection (B)(1)(q)

Claims 162, 163, 171, 267, 268

Subsection (B)(1)(r)

Claims 164, 165, 172, 258, 259

Subsection (B)(1)(s)

Claims 243-268

Subsection (B)(1)(t)

Claims 249-253, 259

Subsection (B)(1)(u)

Claims 254-258, 260, 269-274

Subsection (B)(1)(v)

Claims 251-254, 275-279, 280-285

Subsection (B)(1)(w)

Claims 280-285

Subsection (B)(1)(y)

Claims 280-285

Subsection (B)(1)(z)

Claims 274, 279, 285

Subsection (B)(1)(aa)

Claims 275-279

Subsection (B)(1)(ab)

Claims 280-285

D. The Requirement for Combining Prior Art References to Reject a Claim

In order for different prior art references to be combined to reject a claim the references have to disclose or suggest the combination recited in the claim. ACS Hospitality Systems, Inc. v. Montefiore Hospital, 732 F.2d 1572, 221 USPQ 929 (Fed.Cir. 1984). As the Federal Circuit indicated in the ACS case at 732 F.2d. 1577, 1579, 221 USPQ 929, 933:

"Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention absent some teaching or suggestion supporting the combination. Under Section 103, teaching of references can be combined only if there is some suggestion or incentive to do so."

Neither Barkan nor Zabetian cited by the Examiner in combination to reject a specified number of the claims in this application discloses or suggests certain of the features recited in these claims. The references cannot accordingly be combined to reject the claims.

E. CONCLUSION

All of the claims in this application are allowable over Barkan alone, or the combination of Barkan and Zabetian for all of the reasons discussed above.

Accordingly, reconsideration and allowance of the application are respectfully requested.

Please charge any fee in connection with this amendment to Account No. 06-2425.

Respectfully submitted,
FULWIDER PATTON LEE & UTECHT, LLP

Ellsworth R. Roston
Ellsworth R. Roston
Registration No. 16,310

Howard Hughes Center
6060 Center Drive, Tenth Floor
Los Angeles, CA 90045
Telephone: (310) 824-5555
Facsimile: (310) 824-9696
Customer No. 24201
ERR:dmc